

THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF SOUTH CAROLINA
CHARLESTON DIVISION

IN THE MATTER OF THE SEIZURE OF ALL
FUNDS, MONIES, AND OTHER THINGS OF
VALUE NOT TO EXCEED \$9,800.00
STORED IN OR ACCESSIBLE AT BINANCE
HOLDINGS LIMITED ASSOCIATED WITH
ACCOUNT NUMBER
1Gygq8shDLyNqUDBfpNFv9pDd7X1GRJ8VW

Case No. 2:22-cr-510

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEIZURE WARRANT

I, Special Agent Michael Strobl, your Affiant, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent of the United States Secret Service (USSS) and have been so employed since November 2007. As a Special Agent of the United States Secret Service, I received extensive training at the Federal Law Enforcement Training Center and the James J. Rowley Training Center. This training covered all aspects of financial investigations including money laundering and asset forfeiture, and I have participated in numerous investigations of violations of criminal law including matters involving fraud and white-collar crime.

2. I am submitting this affidavit in support of an application which seeks the issuance of a federal seizure warrant authorizing agents of the United States Secret Service who are involved in the investigation, more particularly described below, to seize the below described account:

All monies, funds, and things of value at Cryptocurrency Exchange Binance Holdings Limited, not to exceed \$9,800.00, held in the account identified by Binance Account Number 1Gygq8shDLyNqUDBfpNFv9pDd7X1GRJ8VW.

Hereinafter referred to as the "Cryptocurrency Account."

3. Your Affiant has probable cause to believe that the funds in the Cryptocurrency Account, described above, are unlawful proceeds of violations relating to Title 18 U.S.C. § 1343 (Wire Fraud) and are thereby subject to civil and criminal forfeiture pursuant to Title 18 U.S.C. § 981(a)(1)(C), made applicable to criminal forfeiture by Title 28 U.S.C. § 2461(c). The funds described herein are also thereby subject to civil and criminal seizure pursuant to Title 18 U.S.C. § 981(b) and Title 21 U.S.C. § 853(e) and (f) by Title 18 U.S.C. § 982(b)(1).

4. This affidavit does not purport to set forth all my knowledge or investigation concerning this case. The statements contained in this affidavit are based on my personal knowledge or from information that I have learned during my investigation, including information from financial institutions, witnesses, and others participating in the investigation.

BACKGROUND ON CRYPTOCURRENCY

5. Based on my training, research, education, and experience, I am familiar with the following relevant terms and definitions as they relate to cryptocurrency:

- a. Cryptocurrency, a type of virtual currency, is a decentralized, peer-to peer, network-based medium of value or exchange that may be used as a substitute for fiat currency to buy goods or services or exchanged for fiat currency or other cryptocurrencies.¹ Examples of cryptocurrency are Bitcoin, Litecoin, and Tether (USDT). Cryptocurrency can exist digitally on the Internet, in an electronic storage device, or in cloud-based servers. Although not usually stored in any physical form, public and private keys (described below) used to transfer cryptocurrency from one person or place to another can be printed or

¹ Fiat currency is currency issued and regulated by a government such as the U.S. Dollar, Euro, or Japanese Yen.

written on a piece of paper or other tangible object. Cryptocurrency can be exchanged directly person to person, through a cryptocurrency exchange, or through other intermediaries. Generally, cryptocurrency is not issued by any government, bank, or company; it is instead generated and controlled through computer software operating on a decentralized peer-to-peer network. Most cryptocurrencies have a “blockchain,” which is a distributed public ledger, run by the decentralized network, containing an immutable and historical record of every transaction.² Cryptocurrency is not illegal in the United States.

- b. Tether (USDT) is a type of cryptocurrency like Bitcoin³ (“BTC”).
- c. Cryptocurrency is stored in a virtual account called a wallet. Wallets are software programs that interface with blockchains and generate and/or store public and private keys used to send and receive cryptocurrency. A public key or address is akin to a bank account number, and a private key is akin to a PIN number or password that allows a user the ability to access and transfer value associated with the public address or key. To conduct transactions on a blockchain, an individual must use the public address (or “public key”) and the private address (or “private key”). A public address is represented as a case-sensitive string of letters and numbers, 26–36 characters long. Each public address is controlled and/or accessed through the use of a unique corresponding

² Some cryptocurrencies operate on blockchains that are not public and operate in such a way to obfuscate transactions, making it difficult to trace or attribute transactions.

³ Since Bitcoin is both a cryptocurrency and a protocol, capitalization differs. Accepted practice is to use “Bitcoin” (singular with an uppercase letter B) to label the protocol, software, and community, and “bitcoin” (with a lowercase letter b) to label units of the cryptocurrency. That practice is adopted here.

private key—the cryptographic equivalent of a password or PIN—needed to access the address. Only the holder of an address’ private key can authorize any transfers of cryptocurrency from that address to another cryptocurrency address.

- d. Although cryptocurrencies such as Bitcoin and Tether have legitimate uses, cryptocurrency is also used by individuals and organizations for criminal purposes such as money laundering and is often used as payment for illegal goods and services. By maintaining multiple wallets, those who use cryptocurrency for illicit purposes can attempt to thwart law enforcement’s efforts to track transactions. As of January 25, 2022, one bitcoin is worth approximately \$36,479.50 though the value of bitcoin is generally much more volatile than that of fiat currencies.
- e. Exchangers and users of cryptocurrencies store and transact their cryptocurrency in a number of ways, as wallet software can be housed in a variety of forms, including on a tangible, external device (“hardware wallet”), downloaded on a PC or laptop (“desktop wallet”), with an Internet-based cloud storage provider (“online wallet”), as a mobile application on a smartphone or tablet (“mobile wallet”), printed public and private keys (“paper wallet”), and as an online account associated with a cryptocurrency exchange. Because these desktop, mobile, and online wallets are electronic in nature, they are located on mobile devices (e.g., smart phones or tablets) or at websites that users can access via a computer, smart phone, or any device that can search the Internet. Moreover, hardware wallets are located on some type of external or removable

media device, such as a USB thumb drive or other commercially available device designed to store cryptocurrency (e.g. Trezor, Keepkey, or Nano Ledger). In addition, paper wallets contain an address and a QR code⁴ with the public and private key embedded in the code. Paper wallet keys are not stored digitally. Wallets can also be backed up into, for example, paper printouts, USB drives, or CDs, and accessed through a “recovery seed” (random words strung together in a phrase) or a complex password. Additional security safeguards for cryptocurrency wallets can include two-factor authorization (such as a password and a phrase). I also know that individuals possessing cryptocurrencies often have safeguards in place to ensure that their cryptocurrencies become further secured in the event that their assets become potentially vulnerable to seizure and/or unauthorized transfer.

- f. Cryptocurrency “exchangers” and “exchanges” are individuals or companies that exchange bitcoin for other currencies and cryptocurrencies, including U.S. dollars and tether. According to Department of Treasury, Financial Crimes Enforcement Network (“FinCEN”) Guidance issued on March 18, 2013, virtual currency administrators and exchangers, including an individual exchanger operating as a business, are considered money services businesses.⁵ Such exchanges and exchangers are required to register with FinCEN and have proper state licenses (if required under applicable state law). From my training

⁴ A QR code is a matrix barcode that is a machine-readable optical label.

⁵ See “Application of FinCEN’s Regulations to Person Administering, Exchanging, or Using Virtual Currencies,” *available at* <https://www.fincen.gov/resources/statutes-regulations/guidance/application-fincens-regulations-persons-administering>.

and experience, I know that registered money transmitters are required by law to follow Bank Secrecy Act anti-money laundering (“AML”) regulations, “Know Your Customer” (“KYC”) protocols, and other verification procedures similar to those employed by traditional financial institutions. For example, FinCEN-registered cryptocurrency exchangers often require customers who want to open or maintain accounts on their exchange to provide their name, address, phone number, and the full bank account and routing numbers that the customer links to an exchange account. As a result, there is significant market demand for illicit cryptocurrency-for-fiat currency exchangers, who lack AML or KYC protocols and often also advertise their ability to offer customers stealth and anonymity. These illicit exchangers routinely exchange fiat currency for cryptocurrencies by meeting customers in person or by shipping cash through the mail. Due to the illicit nature of these transactions and their customers’ desire for anonymity, such exchangers are frequently able to charge a higher exchange fee, often as high as 9–10% (in contrast to registered and BSA-compliant exchangers, who may charge fees as low as 1–2%).

- g. Binance Holdings Limited is a Cryptocurrency exchange and custodian that allows users to buy, sell and store digital assets. They hold a Money Service Business Registration in the United States. Their registration shows an address of Level 3, Melita Court, Triq Giuseppe Cali, Ta’Xbiex XBX 1420, Malta.
- h. Some companies offer cryptocurrency wallet services which allow users to download a digital wallet application onto their smart phone or other digital device. A user typically accesses the wallet application by inputting a user-

generated PIN code or password. Users can store, receive, and transfer cryptocurrencies via the application; however, many of these companies do not store or otherwise have access to their users' funds or the private keys that are necessary to access users' wallet applications. Rather, the private keys are stored on the device on which the wallet application is installed (or any digital or physical backup private key that the user creates). As a result, these companies generally cannot assist in seizing or otherwise restraining their users' cryptocurrency. Nevertheless, law enforcement could seize cryptocurrency from the user's wallet directly, such as by accessing the user's smart phone, accessing the wallet application, and transferring the cryptocurrency therein to a law enforcement-controlled wallet. Alternatively, where law enforcement has obtained the recovery seed for a wallet (see above), law enforcement may be able to use the recovery seed phrase to recover or reconstitute the wallet on a different digital device and subsequently transfer cryptocurrencies held within the new wallet to a law enforcement-controlled wallet.

FACTS SUPPORTING PROBABLE CAUSE

6. On May 13, 2022, your Affiant received a call from Virginia Ogburn-Matthews, a victim of a of an online fraud scheme. Ogburn-Matthews stated that she sent \$9,800 via Bitcoin to an unknown subject she believed worked for Wells Fargo Bank.

7. Law enforcement officers and agents recognize these online fraud schemes as a common way used to describe the illegal activity of receiving help online under false pretenses and then having the victim send money to a bank account of the choosing of the bad actor. This

transferring of funds based on the online fraud scheme is a violation of the federal Wire Fraud statute, 18 U.S.C. § 1343 and the federal Wire Fraud Conspiracy Statute 18 U.S.C. § 1349.

8. Ogburn-Matthews stated that on May 2, 2022, she made contact with an unknown individual after she had clicked on a link for a 1040x tax form. She believed that she was on the IRS website and clicked on legitimate link, but after doing so had a “pop-up” come on the screen to notify her that she had a virus on her computer. As part of the virus protection, it gave a phone number to contact to help clear up the virus. Ogburn-Matthews called the number and spoke to an individual who had “a foreign accent,” which sounded like it was from an individual from India. The unknown individual took her through a few steps over the phone and she allowed him access to her computer via the command prompt. He told her that she had a type of “Trojan” virus called TIMBA, which attacks bank information. At this point, he told her they were on a secure line and that he would be transferring her to an associate of his who works for Wells Fargo, which is the bank that Ogburn-Matthews used.

9. Continuing on May 2, 2022, Ogburn-Matthews spoke with the unknown individual who supposedly worked for Wells Fargo Bank. He told Ogburn-Matthews that there was a pending transaction of a \$9,800 withdrawal from her bank account and there was nothing that could be done to stop it except her go to her bank and withdraw the funds prior to this transaction going through. She should then transfer the money to a secure Bitcoin account and her funds would be safer there. She then went to a National Bitcoin ATM and sent the \$9,800 to address bc1qu3j830xnccj8c9hpnh3pa6ukvw6cxznfl0ha0g (“Address”). Ogburn-Matthews did as instructed because she felt this was the only way to save the funds from being transferred out of her account.

10. On May 13, 2022, your Affiant sent the Address to Kali Schildecker, U.S. Secret Service Criminal Investigative Division, who was able to locate an Account with Binance Holdings Limited associated with the Address. The account number that Schildecker provided was 1Gygq8shDLyNqUDBfpNFv9pDd7X1GRJ8VW (the Cryptocurrency Account identified above).

11. Continuing on May 13, 2022, your Affiant requested the account information for the Cryptocurrency Account to the investigative team at Binance Holdings Limited.

12. Continuing on May 13, 2022, your Affiant spoke with Erin Fracolli, an investigator with Binance Holdings Limited. Fracolli confirmed that the Bitcoin transaction in question was immediately transferred into USDT within this the Cryptocurrency Account. She advised there were 5509.58047857 USDT remaining in the Cryptocurrency Account and that she would freeze the account for 7 days.

13. Fracolli explained that converting Bitcoin to USDT is a common behavior within these schemes.

14. Continuing on May 13, 2022, the Binance financial case team sent an Excel Spreadsheet to SA Strobl with all information regarding the Cryptocurrency Account in question. This spreadsheet included subscriber information, and all account and transaction history within the account. On the dates of the Bitcoin transactions in question, and as described above, the spreadsheet shows transfers of Bitcoin to USDT within the account.

BINANCE HOLDINGS LIMITED ACCOUNT

15. The Binance Holdings Limited account number in question is 1Gygq8shDLyNqUDBfpNFv9pDd7X1GRJ8VW. The account value is currently 5509.58047857 USDT, which is the equivalent of \$5,509.58.

JURISDICTION TO ISSUE OUT-OF-DISTRICT WARRANT

16. Though the Cryptocurrency Account described herein are believed to be located outside the District of South Carolina, 18 U.S.C. § 981(b)(3), as amended by the Civil Asset Forfeiture Act of 2000 (“CAFRA”), Pub. L. No. 106-185, 114 Stat. 202 (2000), explicitly provides jurisdiction for the issuance of seizure warrants for property located in other districts. This statute provides as follows:

Notwithstanding the provisions of Rule 41(a) of the Federal Rules of Criminal Procedure, a seizure warrant may be issued pursuant to this subsection by a judicial officer in any district in which a forfeiture action against the property may be filed under section 1335(b) or Title 28, and may be executed in any district in which the property is found ...

17. Thus, the issuance of the seizure warrant in this district is appropriate under the above statute, as this is the district “in which ... the acts or omissions giving rise to the forfeiture occurred,” based on my training and experience, this is a continuance of a “romance scam” that began with the original victim who is based in Charleston, SC. Further, “venue for the forfeiture action . . . is specifically provided for in section 1395 . . .”. 28 U.S.C. § 1355(b)(1)(A) and (B). Section 1395 provides “for the recovery of a . . . forfeiture . . . in the district where it accrues . . .”.

CONCLUSION

18. I submit that this affidavit supports probable cause for a warrant to seize all funds, monies, and other things of value up to \$9,800.00 stored in or accessible in the Cryptocurrency Account.

19. Based upon the foregoing facts and upon Affiant’s training and experience, there is probable cause to believe that the funds in the Cryptocurrency Account are proceeds traceable to violations of Title 18 U.S.C. § 1343 and subject to civil and criminal forfeiture to the United States pursuant to Title 18 U.S.C. § 981(a)(1)(C) made applicable to criminal forfeiture by Title 28 U.S.C.

§ 2461(c); and are thereby also subject to seizure pursuant to Title 18 U.S.C. § 981(b) and Title 21 U.S.C. § 853(e) and (f) by Title 18 U.S.C. § 982(b)(1).

20. The issuance of the seizure warrant in this district is appropriate under Title 18 U.S.C. § 981(b)(3), and Title 28 U.S.C. § 1355(b)(1) because, notwithstanding the provisions of Rule 41(a) of the Federal Rules of Criminal Procedure, a seizure warrant may be issued by a judicial officer in any district in which a forfeiture action against the property may be filed.

21. Further, a restraining order would not be adequate to preserve the property for forfeiture as the funds in the Cryptocurrency Account can be easily moved, transferred, or dissipated.

22. THEREFORE, your Affiant respectfully requests the issuance of a seizure warrant that will authorize the seizure of funds contained in the Cryptocurrency Account described herein.

23. This affidavit has been reviewed by AUSA Amy Bower.

Respectfully submitted,

Michael Strobl, Special Agent
United States Secret Service

Sworn to me via telephone or other reliable electronic means and signed by me pursuant to Fed. R. Crim. P. 4.1 and 4(d) or 41(d)(3), as applicable on this the 17th day of May, 2022.



Molly H. Cherry
The Honorable Molly H. Cherry
United States Magistrate Judge